International Journal of Computer Science Engineering
and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 3, Issue 5, Dec 2013, 171-176
© TJPRC Pvt. Ltd.

AN EFFICIENT STRUCTURE TO FIND NEW EVASION TECHNIQUES ON NETWORK INTRUSION DETECTION SYSTEM

RUTUJA R. PATIL[1] & P. R. DEVALE[2]

[1]Research Scholar, Department of Information Technology, Bharati Vidyapeeth Deemed, University College of Engineering, Pune, Maharashtra, India

[2]Professor, Department of Information, Technology, Bharati Vidyapeeth Deemed, Pune, Maharashtra, India

ABSTRACT

These days, Signature based Network Intrusion Detection Systems (NIDS), which apply a set of rules to identify hostile traffic in network segments are quickly updated in order to prevent systems against new attacks. The objective of an attacker is to find out new evasion techniques to stay unseen. Unfortunately, majority of the existing techniques are based on the ambiguities of the network protocols. As a result of the emergence of the new evasion techniques, NIDS system may fail to give the correct results. The central idea of our paper is to develop a network based intrusion detection system based on Apriori algorithm and other approaches for attack detection and test the input thus produced by the Apriori algorithm with the well known snort intrusion detection system, once candidate sets for detecting different attacks are generated. These candidates in turn will be passed as inputs to the snort intrusion detection system for detecting different attacks.

KEYWORDS: NIDS, Evasion, Apriori Algorithm, Adaboost Algorithm, Snort

INTRODUCTION

Information Technology systems have become a critical component in organizations that manage a huge personal and critical data. Guarding those systems from hostile actions should be the main goal when applying security measures. Intrusion Detection System (IDS) are becoming more and more widely deployed to supplement the security provided by firewalls. IDS function in the digital world much the same way as a burglar alarm does in the physical world. Like all alarms, IDS also have certain flaws that can be exploited by an attacker to get around the system. The conflict between the attackers and IDS developers is never ending. Attackers continually try to find new exploits to intrude a system, while system developers attempt to analyse and detect attacks.

Intrusion Detection System

To understand what is a network intrusion detection system one should first know what intrusion is. When a hacker tries to make way into your system, it is known as intrusion. An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. Intrusion Detection System can be classified in different ways. The major classifications are Network based (NIDS) and host based (HIDS) intrusion detection systems.

Network Based Intrusion Detection System

The word network is used for this system, because it keeps an eye on packets on a network wire and its main objective is to find out whether a cracker or a hacker is breaking into your system. It analyzes the traffic on your network to monitor signs of different malicious activity.

A network intrusion detection system is mostly place at strategic points in a network, so that it can monitor the traffic travelling to or from different devices on that network. [3]

These systems can be broadly classified into two major categories. These are mainly: i) Anomaly based NIDS(ii) Signature based NIDS. In this paper, we focus on Signature based NIDS.

Signature Based Intrusion Detection System

A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from known malicious threats. This is similar to the way most antivirus software detects malware. The issue is that there will be a lag between a new threat being discovered and the signature for detecting that threat being applied to your IDS[2]. During that lag time your IDS would be unable to detect the new threat.

This situation causes attackers to focus in finding evasions over the signatures of these systems. The overall idea of an intruder is to undertake an attack in such a way that it remains undetected by the Intrusion Detection system. Typically, an attacker has to know how an IDS reacts to certain attack patterns; the attacker then changes these patterns so that the attack blends in with the rest of the traffic and thus remains undetected.

Following is the simplified explanation of Evasion:

Let us consider that the words “ attack “ and “ intrude “ represent two strings of known malicious code. When an IDS identifies those strings in the request, the system intervenes and denies entry.

If, however, “ kaarindtuettcr “ and“tittnrrakdeuac “ were part of a request, the system would not recognise the code as simply being the well known malicious strings “ attack “ and “ intrude “ combined and rearranged in a new way. The IDS would not intervene and entry would be allowed.

The aim of this paper is to look for new evasive techniques by analysing NIDS behaviour. In this approach initially we build NIDS using c4.5 algorithm. KDD – 99, publicly available dataset is given to it. Ada Boost Algorithm is applied for supervised learning where labelling of dataset is done as normal or attack. Apriori algorithm generates rules which are checked on Snort for evasion.

LITERATURE SURVEY

In this section, we review the evasion techniques and the evasion tools.

Evasion Techniques

The comman evasion techniques are as follows:

- **Denial-of-Service**: Its purpose is to overwhelm network bandwidth or system resources such as the CPU, memory space, peripherals. It generates a large volume of network traffic.[3]
- **Packet Splitting**: It includes IP fragmentation and TCP segmentation, it splits IP datagrams or TCP stream into non overlapping fragments or segments specially small ones. If an IPS does not completely reassemble the IP fragments or TCP segments to restore the original application content, it may neglect an attack embedded in the content which is targeted at the victim host.
- **Duplicate Insertion**: It is a technique in which attackers insert duplicate or overlapping segments to confuse the IDS. For Example : the attacker could send packets whose Time To Live fields have been crafted to reach the IDS but not the target computers it protects.[3]

- **Payload Mutation**: It means an attacker transforms malicious packet payloads into semantically equivalent ones. The transformed payloads will look different from the signatures that an IPS expects, so that the attack can evade detection.

Evasion Tools

Fragroute intercepts, modifies, and rewrites egress traffic destined for the specified host. It implements packet splitting and duplicate insertion at the TCP/IP layer and helps the attackers evade signature matching on the NIDS. The attackers can write a simple script to arrange the sequence of evasion techniques to be launched before running. Fragroute, which then automatically transforms attack traffic into the specified format to cheat the IDS.[1]

Niktois a web scanning tool for generating multiple malicious URI requests. It helps developers and network administrators to test their Web servers for possible security problems.[1]

Havij is an automated SQL injection tool to exploit SQL injection vulnerabilities on web pages. It supports evasion by manipulating white spaces in the attack strings, replacing space with the comment syntax of the C language.

AD Mutate is an engine for shellcode mutation that helps an attack program to evade IDS. The engine casn obfuscate the appearance of a piece of shellcode but retain its effectiveness to exploit a software vulnerability.

Sploit is an evasion testing framework that allows the testers and attackers to develop new attacks and evasion techniques.

Idsprobe takes as input a packet trace and from it constructs a configurable set of variant traces that introduce different forms of ambiguities that can lead to evasions.[2]

Protocol Scrubbers which are transparent interposed mechanisms for explicitly removing network scans and attacks at various protocol layers.[2]

Split-Detect which focus on the simplest form of signature, an exact string match and start by splitting the signature into pieces.

Snort is a lightweight, freely available Intrusion Detection. In Snort, network topologies and the interpretation policy of the endpoint being monitored with the help of real time alerting capability. The idea of this paper comes from, where GP was used to model a simple NIDS with great accuracy, using a publicly available Lawrence Berkley National Laboratory (LBNL) dataset. Later paper present new improvements, performing evasions over that NIDS and corroborating the effectiveness of modeling NIDS with GP using another publicly available set KDD-99. Adaptive IDS audit data so that abnormal intrusive activities can be detected by comparing the current activities with the profile.

PROPOSED SYSTEM

The main aim of this paper is to develop a network based intrusion detection system based on modified Apriori approach for attack detection and test the input thus produced by the Apriori algorithm with the well known snort intrusion detection system, once a candidate sets for detecting different attacks are generated. These candidates in turn will be passed as inputs to the snort intrusion detection system for detecting different attacks. In figure 1 the proposed system flow is given where, the input to C4.5 algorithm using Weka tool. Weka tool is implementation of various classifying and clustering algorithm[8]. C4.5 algorithm gives output as a decision tree. The workflow is depicted in the following block diagram.

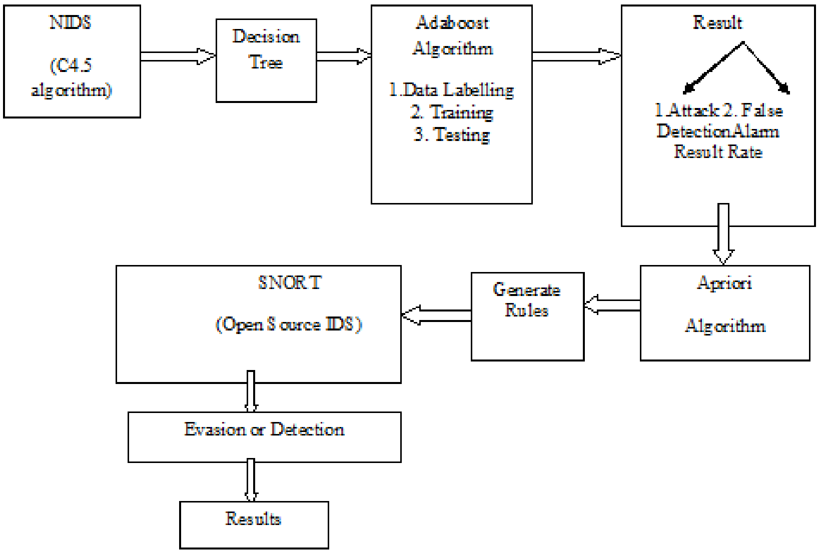

Figure 1: Flow of System

After that, adaboost algorithm is applied on output of C4.5. Adaboost algorithm contains steps like data labeling, training and testing. Data labeling will contain identification normal and attack packets. +1 means attack packet and -1 means normal packet. Training phase will contain initialization of parameters. Testing phase will contain real identification attack packets and classifying each detected attack under its category (Such as Dos attack, probe attack, U2R attack, R2Lattack). After that detection result and false alarm rate will get displayed. After this step modified apriori algorithm is used, which contain process of creation of rules for detecting attacks. After creating rules they are passed to snort. Snort is an open source IDS. Now this method will detect the packets in the network. It evades the packets by changing the rules[5]. Detection output will get stored in text files.

CONCLUSIONS AND FUTURE WORK

This paper provides a new method that efficiently improves the task of finding out new forms of evasion by analysing NIDS behaviour thus allowing system administrators to be warned before the attackers could exploit them.

The aim of evasion is not to break the NIDS system but to understand and learn different ways of evasion of system and make system more sturdier. We have two main objectives for incoming work. First is to create our own dataset as in this paper we are using KDD – 99, publicly available dataset. The other objective is to analyse if these techniques can be applied to real time NIDS.

REFERENCES

1. T. H. Ptacek and T. N. Newsham, "Insertion, evasion and denial of service: Eluding network intrusion detection," Technical report, 1998.

2. S. Pastrana, A. Orfila, A. Ribagorda, “A Functional Framework to Evade Network IDS”, IEEE xplore, System Sciences (HICSS), 2011 44th Hawaii International Conference.

3. S. Peddabachigaria, A. Abraham, “Modeling intrusion detection system using hybrid intelligent systems”, Journal of Network and Computer Applications.

4. Pallavi Dhade, T. J. Parvat, “To Evade Deep Packet Inspection in NIDS Using Frequent Element Pattern Matching”, IJEIT, Volume 2, Issue 1, July 2012

5. M. Roesch, "Snort - Lightweight Intrusion Detection for Networks," in LISA '99: *13th USENIX conference on System administration, Seattle, Washington,* 1999, pp. 229--238.

6. F. Bodon. “A Fast Apriori Implementation”. *IEEE ICDM Workshop on Frequent Itemset Mining Implementations,* 2003.

7. S. Pastrana, A. Orfila, and A. Ribagorda, “Modeling NIDS evasion with Genetic Programming”, *International Conference on Security and Management, SAM 2010, Las Vegas, Nevada, USA*, July 11-15, 2010

8. M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, I. H. Witten, "The WEKA Data Mining Software: An Update", in SIGKDD Explorations, Volume 11, Issue 1, 2009